Misbruik van technische hulpmiddelen

Koops, E.J.; Prins, J.E.J.

Published in:
Computerrecht

Publication date:
2004

Koops, B.J. & Prins, J.E.J. (2004). Misbruik van technische hulpmiddelen: een beschouwing over de te ver gaande regelingen in het Cybercrime-verdrag en de Auteursrechtenrichtlijn. Verschenen in: *Computerrecht*, 59-67.

Misbruik van technische hulpmiddelen: een beschouwing over te vergaande regelingen in het Cybercrime-Verdrag en de Auteursrechtrichtlijn

B.J. Koops, J.E.J. Prins[1]

1. Inleiding

Naar verwachting zullen dit jaar de laatste stappen worden gezet in de parlementaire behandeling van het wetsvoorstel ter aanpassing van de Auteurswet aan de Europese Richtlijn auteursrecht in de informatiemaatschappij (Auteursrechtrichtlijn). Als alles volgens plan verloopt zullen verder stappen worden gezet voor de implementatie van het Cybercrime-verdrag van de Raad van Europa. Alhoewel beide regelingen op het eerste gezicht twee geheel verschillende domeinen bestrijken, laat een nadere beschouwing zien dat er ook overeenkomsten zijn. Beide instrumenten kennen namelijk een regeling waarin het misbruik van technische hulpmiddelen aangepakt wordt.

Deze wettelijke regulering van technische hulpmiddelen lijkt niet op zichzelf te staan. Het beeld dat in onze huidige informatiemaatschappij opkomt is dat van een verregaande invloed van technologie op regulering. Bekende voorbeelden zijn filterprogramma's en *digital rights management*-systemen. Ook buiten het domein van ICT blijkt inmiddels uit een scala aan toepassingen dat technologie een belangrijke bijdrage kan leveren aan het handhaven van wet- en regelgeving. Maar technologie biedt ook interessante mogelijkheden om technische handhavingsinstrumenten vervolgens weer te ontduiken. Bekend zijn radarverklikkers die automobilisten waarschuwen voor radarsignalen van snelheidscontroles en laserschilden die de auto met een waas van infrarode straling omringen waardoor de politie niet langer kan vaststellen hoe hard iemand rijdt. Juist omdat blijkt dat handhavingstechnologieën op hun beurt weer vatbaar zijn voor omzeiling, zetten wetgevers in op het aanpakken van omzeilingsfaciliteiten. Zo kennen we in ons land sinds 1 januari 2004 een regeling die het gebruik van radarverklikkers strafbaar stelt.[2]

De regelingen in het Cybercrime-Verdrag en de Auteursrechtrichtlijn kenmerken zich door een vergaande aanpak van misbruik van hulpmiddelen. Nu kent ons land al langer wettelijke regelingen waarin het misbruik van hulpmiddelen verboden is, maar de regeling in het Cybercrime-Verdrag lijkt aanzienlijk verder te gaan dan huidige strafrechtelijke aansprakelijkstellingen. Ook de Auteursrechtrichtlijn lijkt de vertrouwde ankerpunten voor aansprakelijkstelling op de tocht te zetten. En alhoewel de voorgestelde auteursrechtregeling nu weliswaar een civielrechtelijke sanctie kent, heeft de wetgever aangegeven te bezien hoe de regeling zich verhoudt tot de strafrechtelijke normering van art. 6 van het Cybercrime-verdrag.

In dit artikel willen we de beide regelingen op het terrein van ICT plaatsen tegen de achtergrond van het systeem van strafrechtelijke aansprakelijkstelling. Hiermee beogen wij de vraag te beantwoorden of de lopende ontwikkelingen rondom technologische hulpmiddelen passen

[1] Bert-Jaap Koops is universitair hoofddocent recht en techniek bij het Centrum voor Recht, Bestuur en Informatisering van de Universiteit van Tilburg (www.uvt.nl/ crbi). Corien Prins is hoogleraar recht en informatisering bij hetzelfde centrum. Dit artikel is een bewerking van een eerdere bijdrage, getiteld 'De toenemende strafbaarstelling van technische hulpmiddelen: over intenties, bestemmingen en instrumentele wetgeving', opgenomen in de bundel *Glijdende Schalen, liber amicorum J. de Hullu*, (red. M.S. Groenhuijsen & J.B.H.M. Simmelink), Nijmegen: Wolf Legal Publishers, 2003, p. 341-386.

[2] Besluit van 3 november 2003, houdende wijziging van het Voertuigreglement tot opneming van een verbod voor radarontvangstapparaten, Stb. 2003, 464.

binnen het systeem van de wet en of zij aanvaardbaar zijn in het licht van de grondslagen van het materiële strafrecht.

2. Strafbaarstelling van hulpmiddelen in het systeem van het materiële strafrecht[3]

2.1. De positie van hulpmiddelen in strafwetgeving

Ons recht kent diverse strafbaarstellingen rond hulpmiddelen. Gewezen kan worden op bepalingen inzake geld- of waardepapiervervalsing en de recentelijk weer in de belangstelling staande bepaling over het voorbereiden van misdrijven tegen de staatsveiligheid (die in het 'Jihad-proces'[4] werden ingezet). Verder bevat art. 46 Sr een algemene regeling waarin voorbereidingshandelingen strafbaar zijn gesteld.[5] Deze regeling is overigens wel beperkt tot zeer ernstige misdrijven en tot het gebruik van hulpmiddelen, een geobjectiveerde concretisering van het abstracte 'voorbereiding'. Hoewel de hulpmiddelen en de gedragingen limitatief zijn opgesomd, levert dat geen substantiële beperking op: onder andere vrouwenpruiken, dameskleding, cosmetica en plastic patatvorkjes fungeren als art. 46-voorbereidingsmiddelen.[6] De crux van de strafbaarstelling lijkt daarom te liggen op de kennelijke bestemming van de middelen.
Ook op het terrein van ICT kennen we strafbaarstellingen rond hulpmiddelen. Art. 32a Auteurswet bepaalt dat het opzettelijk ter verspreiding aanbieden of voorhanden hebben, het invoeren, doorvoeren of uitvoeren, of het bewaren uit winstbejag van softwarekraakmiddelen strafbaar is. Daarbij moet het wel gaan om middelen die *uitsluitend* bestemd zijn om programmatuurbeveiliging te kraken. Een middel dat ook andere doeleinden heeft, valt dus niet onder de strafbaarstelling. Art. 326c lid 2 Sr stelt strafbaar handelingen met apparatuur voor het kraken van systemen waarmee zonder te betalen gebruik kan worden gemaakt van telefonie of betaal-tv.
De bijzondere strafbaarstellingen van voorbereidingshandelingen hangen samen met fundamentele rechtsgoederen van algemeen belang: de integriteit van de economie (bij vervalsingsdelicten), de volksgezondheid en de staatsveiligheid. De strafbaarstelling van ICT-hulpmiddelen kent wat dat betreft een minder in het oog springend rechtsgoed: softwarekraakmiddelen en telecomfraude bedreigen onderdelen van de economie, maar niet de integriteit van de economie zelf.[7]
De strafbaarstellingen van hulpmiddelen staan op gespannen voet met ons 'daadstrafrecht': strafrechtelijke aansprakelijkheid ontstaat in principe slechts bij waarneembare, strafwaardig te achten gedragingen.[8] Wij gaan ervan uit dat het Nederlandse strafrecht nog steeds een daadstrafrecht is: in beginsel worden alleen strafwaardig geachte gedragingen strafbaar gesteld. Bestaande uitzonderingen zijn niet bedoeld om dit uitgangspunt te verlaten.[9]

---

[3] Voor een uitgebreidere behandeling, zie Koops & Prins, *a.w.*, noot 1.
[4] Rb. Rotterdam 5 juni 2003, rechtspraak.nl, LJN-nummer AF9546.
[5] Stb. 1994, 60. In 2001 (Stb. 2001, 675) zijn hieruit de woorden 'in vereniging' geschrapt, waardoor het bereik aanzienlijk is uitgebreid.
[6] Peter Smith, *Strafbare voorbereiding. Een rechtsvergelijkend onderzoek*, diss. Groningen, CRBS-dissertatiereeks, 2003, p. 44n.
[7] Volgens de Hoge Raad is de ratio van art. 326c lid 2 Sr 'een doelmatige bescherming van het economische belang van de verschaffing van telecomdiensten'. HR 15 april 2003, rechtspraak.nl, LJN-nummer AF3372.
[8] J. de Hullu, *Materieel strafrecht. Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht*, Deventer: Gouda Quint 2000, p. 372.
[9] Vgl. Remmelink, *Mr. D. Hazewinkel-Suringa's Inleiding tot de studie van het Nederlandse Strafrecht*, Arnhem: Gouda Quint 1995, p. 100: 'Men is het er in Nederland wel over eens, dat strafbaarstelling van voorbereidingshandelingen gelet op de evidente rechtsstatelijke bezwaren tot een minimum beperkt dient te worden.'

2.2. Het systeem en redenen voor uitzonderingen

Vanuit het basisidee van een daadstrafrecht, kunnen we de bestaande strafbaarstellingen rond hulpmiddelen plaatsen. We presenteren onderstaand allereerst een tweetal categorieën strafbaarstellingen en vervolgens een viertal redenen waarom het strafrecht niet altijd volstaat met strafbaarstelling van strafwaardige handelingen zelf. Deze onderscheidingen zullen bij de latere analyse van de ICT-gerelateerde bepalingen inzake hulpmiddelen als toetsingskader fungeren.

Een eerste categorie past naadloos binnen het systeem: dit betreft voorbereidende gedragingen die op zichzelf als strafwaardig kunnen worden gezien. In de zuiverste vorm komt deze categorie nauwelijks voor. Het invoeren of uitvoeren van vervalst geld (art. 209 Sr) kan wellicht gezien worden als een inherent strafwaardige gedraging, maar er zijn verder nauwelijks voorbeelden te bedenken waarin een voorbereidende gedraging niet ook een legitiem doel zou kunnen hebben.
De tweede categorie strafbaarstellingen betreft uitzonderingen op het uitgangspunt van daadstrafrecht. Het zijn strafbaarstellingen van gedragingen die op zichzelf niet strafwaardig zijn, maar die dusdanig ingrijpende gevolgen kunnen hebben dat niet volstaan kan worden met het afwachten van die gevolgen. Er kunnen verscheidene redenen zijn om een dergelijke uitzondering in te voeren.
Een eerste reden is wanneer een gedraging bijna onvermijdelijk leidt tot het plegen van een strafbaar feit; deze gedraging zelf wordt dan aangepakt in plaats van het latere strafbare feit. De tweede reden betreft de ingrijpendheid van de gevolgen. Gedragingen die op zichzelf niet strafwaardig zijn maar die kunnen leiden tot zeer ernstige gevolgen, worden strafbaar gesteld, omdat de strafbaarstelling van het gevolg zelf onvoldoende (b)lijkt. De ontoereikendheid van strafbaarstelling van het gronddelict kan liggen in het gevaarzettende karakter van het gronddelict: het maatschappelijke belang van ingrijpen vóórdat de gevolgen (de brand, het kindermisbruik) zich voordoen weegt dan zwaarder dan het uitgangspunt dat het strafrecht reactief is. Deze ratio ligt ten grondslag aan diverse bijzondere strafbaarstellingen.
De ontoereikendheid kan evenwel ook liggen in praktische problemen bij de handhaving, een derde reden voor uitzonderingen op het daadstrafrecht. Indien het gronddelict dermate moeilijk is op te sporen of te vervolgen dat de strafbaarstelling illusoir wordt, is het aanvaardbaar om een voorbereidingshandeling die wél goed is op te sporen strafbaar te stellen. Dit kan mede een reden zijn geweest, hoewel niet expliciet uitgesproken, voor bijvoorbeeld de strafbaarstelling van hulpmiddelen bij geldvervalsing en zware drugsdelicten.
Tot slot speelt volgens ons nog een vierde reden mee waarom het strafrecht niet altijd volstaat met strafbaarstelling van strafwaardige handelingen zelf: de signaalwerking van wetgeving. Om de strafwaardigheid van bepaalde handelingen te benadrukken, kan het aangewezen zijn om gedragingen in de periferie daarvan eveneens strafbaar te stellen. Omdat in bepaalde kringen het ontduiken van betaling voor telefonie als sport werd gezien, is ter ontmoediging van deze subcultuur niet alleen het ontduiken zelf strafbaar gesteld, maar ook het verspreiden van middelen die daarvoor kunnen worden gebruikt (art. 326c lid 2 Sr).

2.3. Aanknopingspunten voor strafbaarstelling bij hulpmiddelen

Als laatste stap in onze algemene analyse zetten wij op een rijtje wat de aanknopingspunten zijn van de bestaande uitzonderingen op het daadstrafrecht. Op welke manieren worden niet-strafwaardige gedragingen strafbaar gesteld?
Het eerste aanknopingspunt is het hulpmiddel zelf. Soms wordt dit algemeen aangeduid ('middelen', art. 32a Aw), vaak worden meer of minder uitgebreide aanduidingen en opsommingen gehanteerd van mogelijke hulpmiddelen: 'stoffen of voorwerpen' (art. 214, 223, 234 Sr), 'voorwerpen' (art. 96 lid 2 onder 3 Sr), of 'voorwerpen, stoffen, informatiedragers, ruimten of vervoermiddelen' (art. 46 Sr). De aanduidingen zijn steeds zo veelomvattend, dat zij nauwelijks een beperking inhouden – alleen gegevens vallen er niet onder.
Daarom is het tweede aanknopingspunt belangrijker: de bestemming van het middel. Deze bestemming kan intrinsiek of extrinsiek worden afgeleid. Sommige hulpmiddelen hebben bijna

naar hun aard een zuiver misdadig karakter (vals geld, art. 209 Sr), maar de meeste hebben intrinsiek een tweeledig karakter: ze kunnen zowel voor misdadige als voor legitieme doeleinden worden gebruikt. Vrijwel alle bepalingen gaan over deze laatste categorie: vaak betreft het alledaagse voorwerpen en middelen. Een intrinsieke bestemming van het hulpmiddel is daarom zelden aan de orde. Het tweede aanknopingspunt omvat dan ook vooral extrinsieke factoren die de bestemming van een hulpmiddel bepalen. Hierbij worden verschillende modaliteiten gehanteerd, zoals 'een voorwerp dat bestemd is', 'een middel dat bestemd of gebruikt is', 'een voorwerp dat kennelijk bestemd is' dan wel 'een voorwerp dat geschikt is' of 'een middel dat kan dienen'. De bepalingen laten hierbij in het midden uit welke extrinsieke factoren moet of kan blijken dat een middel in concreto bestemd is voor een strafbaar feit. Wel wordt een onderscheid gemaakt tussen de daadwerkelijke bestemming in concreto ('bestemd') en een geobjectiveerde bestemming ('kennelijk bestemd').[10] Bij de eerste categorie zal de rechter meer subjectieve factoren moeten betrekken dan bij de tweede.
Het derde aanknopingspunt haakt aan bij deze subjectieve invulling: in hoeverre moet de dader weet hebben van de (misdadige) bestemming? Meestal is expliciete kennis nodig: 'waarvan hij weet dat zij bestemd zijn'. Soms is sprake van een verlaagde eis, namelijk de geobjectiveerde bestemming: 'kennelijk bestemd' (art. 46, 326c Sr).
Naast de hulpmiddelen zelf, wordt ook aangegrepen bij de handelingen die met die middelen worden gepleegd. Een vierde aanknopingspunt is dan ook welke handelingen met de middelen gepleegd worden, bijvoorbeeld het verwerven, vervaardigen, invoeren, doorvoeren, uitvoeren of voorhanden hebben (art. 46) of het openlijk ter verspreiding aanbieden, ter verspreiding voorhanden hebben, invoeren, doorvoeren, uitvoeren, of uit winstbejag bewaren (art. 32a Aw). De bepalingen kunnen hierbij worden onderverdeeld in marktgerichte (of commerciële) gedragingen (invoeren, uitvoeren, openlijk ter verspreiding aanbieden, ter verspreiding voorhanden hebben, uit winstbejag vervaardigen of bewaren) en in persoonsgerichte gedragingen (voorhanden hebben, bij zich hebben, verwerven, vervoeren).
Opmerkelijk is dat het vervaardigen slechts op twee plaatsen is strafbaar gesteld: bij de algemene voorbereidingshandelingen (art. 46 Sr) en bij de geldvervalsingmiddelen (art. 214 Sr). Bij telecomfraudemiddelen is de vervaardiging alleen strafbaar gesteld als dit uit winstbejag geschiedt; bij de softwarekraakmiddelen is zelfs dat niet gebeurd. Over het algemeen wordt dus eerder aangeknoopt bij markthandelingen dan bij het vervaardigen van middelen.
Bij de handelingen rond hulpmiddelen speelt tot slot nog het vijfde aanknopingspunt een rol: het opzet van de verdachte op het plegen van een gronddelict. De gedraging moet meestal plaatsvinden met het opzet een gronddelict te plegen, maar soms is er ook een opzeteis zonder relatie tot een gronddelict (art. 32a Aw). Een enkele keer ontbreken zelfs zowel opzeteis als relatie met een gronddelict (art. 214, 223, 234 Sr). Dit laatste is bijzonder, omdat hier de causale relatie met de strafwaardige gedraging is losgelaten: de 'voorbereiding' wordt in zichzelf strafbaar gesteld, zonder dat in concreto sprake hoeft te zijn van een voorbereiding tot een strafbare handeling.

3. Nieuwe strafbaarstellingen van technische hulpmiddelen

Nu we in het voorgaande de relevante aanknopingspunten voor strafbaarstelling van hulpmiddelen uiteen hebben gerafeld, is het interessant te bezien hoe twee nieuwe ICT-gerelateerde voorbeelden van aansprakelijkstelling zich hiertoe verhouden.

[10] Smith is van oordeel dat 'kennelijk bestemd' betekent dat de bestemming in concreto bestond en dat deze bestemming op enigerlei wijze duidelijk moet zijn (Smith, *a.w.*, noot 6, p. 47). Volgens ons is 'kennelijk' juist een afzwakking, geen versterking, en hoeft de bestemming niet in concreto te hebben bestaan maar alleen – voor anderen – aannemelijk te zijn op basis van het geheel van omstandigheden.

Koops, B.J. & Prins, J.E.J. (2004). Misbruik van technische hulpmiddelen: een beschouwing over de te ver gaande regelingen in het Cybercrime-verdrag en de Auteursrechtenrichtlijn. Verschenen in: *Computerrecht*, 59-67.

3.1. Kraakmiddelen en het Cybercrime-verdrag

In november 2001 is het Cybercrime-Verdrag (CCV) van de Raad van Europa ondertekend door dertig landen, waaronder Nederland.[11] Art. 6 CCV stelt, kort gezegd, hulpmiddelhandelingen strafbaar die worden gepleegd met het doel een cyberdelict te plegen. Het gaat in art. 6 dus om bijvoorbeeld het ontwikkelen, beschikbaar stellen of voorhanden hebben van apparatuur of programmatuur voor hacken, gegevensmanipulatie en virusverspreiding, gegevensonderschepping of computersabotage. Ook het voorhanden hebben van wachtwoorden of toegangscodes waarmee toegang tot een computer(systeem) kan worden verkregen, is strafbaar als men van plan is om daarmee bijvoorbeeld computervredebreuk te plegen. Beschikbaar stellen wordt breed uitgelegd: het gaat bijvoorbeeld om het op het Internet plaatsen voor het gebruik door anderen, maar dit omvat zelfs het opnemen van (een lijst met) hyperlinks die opzettelijk de toegang tot hulpmiddelen faciliteren (MvT, §72). De primaire gedachte achter deze strafbaarstelling is de vrees voor een zwarte markt voor hackersmiddelen en dergelijke: de bepaling dient om een dergelijke zwarte markt effectiever te bestrijden (MvT, §71). In de voorbereiding van het verdrag is vooral veel gediscussieerd over de mate waarin de hulpmiddelen een illegale bestemming moeten hebben. Als 'reasonable compromise' is gekozen voor een beperking tot 'devices [that] are objectively designed, or adapted, *primarily* for the purpose of committing an offence' (MvT, §73, onze cursivering). Men is zich hierbij wel bewust geweest van het gevaar van 'overcriminalisation' voor hulpmiddelen die op de markt worden gebracht voor legitieme doeleinden. Daarom is, naast het hoofdzakelijke doel van het middel zelf, een specifiek opzetvereiste toegevoegd aan de handeling met het hulpmiddel: deze handeling dient ook te geschieden met het doel om een misdrijf te plegen (MvT, §76).
Voorts zijn er nog enkele spijtopties voor verdragspartijen ingebouwd. Een verdragspartij heeft, aldus art. 6 lid 3, de mogelijkheid om een voorbehoud te maken bij dit artikel, maar zij moet in elk geval wel de verkoop, verspreiding en het beschikbaarstellen van een wachtwoord of toegangsgegevens strafbaar stellen (MvT, §78).

Beoordeling
Hoe past de strafbaarstelling van cybercriminaliteitshulpmiddelen in het Nederlandse strafrecht? De toelichting geeft als ratio voor strafbaarstelling de noodzaak van het voorkomen of bestrijden van een zwarte markt voor hulpmiddelen, met als argument gevaarzetting van de voorbereidingshandelingen. Dit lijkt ons een slecht argument voor strafbaarstelling: elke voorbereidingshandeling tot een strafbaar feit is gevaarzettend doordat het voorbereidt op dat strafbare feit. Aldus zou elke voorbereidingshandeling strafbaar zijn te stellen. Een substantiëler argument kan zijn dat de delicten van art. 2-5 CCV dermate gevaarzettend zijn – zijnde een aantasting van het belangrijke rechtsgoed van de integriteit van de informatie-infrastructuur – dat de voorbereiding ervan in een vroeg stadium moet worden aangepakt. Echter, sommige feiten, zoals computersabotage, zijn ernstig en hebben een dergelijk gevaarzettend karakter, maar andere zijn betrekkelijk onschuldig, zoals het veranderen van gegevens in een pc. Differentiatie is daarom volgens ons eerder aangewezen dan integrale strafbaarstelling.

[11] Verdrag inzake de bestrijding van strafbare feiten verbonden met eleketronische netwerken, Trb. 2002, 18. Het verdrag treedt in werking zodra vijf staten (waaronder drie RvE-staten) het hebben geratificeerd; in januari 2004 hadden Albanië, Kroatië, Estland en Hongarije dat gedaan. Op <http:/ / conventions.coe.int/ Treaty/ EN/ WhatYouWant.asp?NT= 185> vindt men de tekst van het verdrag, het toelichtend rapport en een ratificatieoverzicht. Een uitvoerige bespreking van het verdrag biedt Kaspersen in: Rik Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: J.E.J. Prins e.a. (red.), *Recht & Informatietechnologie* (losdelig), Den Haag: Sdu, augustus 2002. Op het moment van schrijven (februari 2004) is nog geen wetsvoorstel voor ratificatie van het verdrag of voor implementatie in Nederland beschikbaar. Verwacht wordt dat de implementatie in de loop van dit jaar beslag krijgt. Zie ook B.J. Koops, 'Het Cybercrime-verdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij', *Computerrecht* 2003/ 2, p. 115-123.

De vormgeving van de bepaling zelf is ook verstrekkend in bepaalde opzichten. In de eerste plaats is de opsomming van hulpmiddelen uitgebreid, aangezien het niet alleen programmatuur en apparatuur omvat, maar ook wachtwoorden en toegangscodes. Nu kan verspreiding van toegangscodes ernstige computercriminaliteit in de hand werken, maar het kan ook betrekkelijk onschuldige handelingen betreffen als het verstrekken aan een collega van een wachtwoord om een beveiligde Internetpagina te raadplegen (hetgeen dan 'illegal access', art. 2 CCV, zou kunnen opleveren). Veel kranten op het Internet zijn bijvoorbeeld alleen toegankelijk met een wachtwoord na gratis registratie. Mede gezien de brede uitleg van 'verstrekken' (zie onder), kan men zich afvragen of de strafbaarstelling hier niet te ver voert.
Een belangrijk punt is voorts de bestemming van het hulpmiddel. Het gaat om middelen die *vooral ontworpen of aangepast* zijn om delicten te plegen. Of dat bewijsproblemen daadwerkelijk voorkomt, zoals de bedoeling is, is nog maar de vraag. De toelichting stelt dat het moet gaan om '*objectively* designed or adapted' (§73, onze cursivering): het ontwerpdoel moet geobjectiveerd aantoonbaar zijn. Maar hoe valt dit te bewijzen?
Een mogelijkheid is te kijken naar de toepassingsmogelijkheden van een middel: voor welke toepassingen kan dit in beginsel worden gebruikt? Dit is echter nauwelijks te bepalen, en zeker niet uitputtend; bovendien is altijd wel ergens een legitieme toepassing te vinden. En wat betekent 'primarily' dan: is een hulpmiddel strafbaar als het voor 95% illegale toepassingen heeft, of voor 80%, of voor 60%? De toelichting geeft aan dat deze clausule 'will usually exclude dual-use devices' (MvT, §73), maar 'usually' is even rekbaar als 'primarily'.[12]
Wordt het ontwerpdoel wellicht afgelezen aan de achtergrond van de maker, zodat door (respectabele?) bedrijven ontwikkelde middelen worden aangenomen een legale bestemming te hebben, maar door individuele (*nerd*-achtige?) computergekken ontwikkelde middelen vermoed worden een illegale bestemming te hebben? Dat doet volgens ons geen recht aan de diversiteit in de motoren van het Internet: juist de *nerds*, de individuen, de kleine bedrijfjes hebben vaak de technologie ontwikkeld van en voor het Internet. Het is ook mogelijk dat de bestemming zal worden afgeleid uit het gebruik: indien een middel 'primair' wordt gebruikt voor illegale doelen, zal het wel een illegaal ontwerpdoel hebben. Maar ook dat doet niet echt recht aan het Internet: als uit onderzoek zou blijken dat beschrijfbare cd's voor 80% worden gebruikt voor het ongeautoriseerd copiëren van muziek, geeft dat een beschrijfbare cd dan een illegaal doel?
Aldus bestaat het gevaar dat de strafbaarstelling van 'primair illegale' hulpmiddelen een schaduw van strafbaarheid vooruit gaat werpen en mogelijk een verkillend effect zal hebben op onderzoek naar en ontwikkeling van technologie. Bij de implementatie zal de Nederlandse wetgever zich hier rekenschap van moeten geven, en indien hij gebruikmaakt van vergelijkbare termen, zal hij scherp moeten toelichten hoe bepaald wordt wanneer een hulpmiddel primair is ontworpen voor het plegen van een computerdelict.[13]

Een volgend aspect van art. 6 CCV is de opsomming van gedragingen. Ondanks de titel, 'Misuse of devices', wordt hier niet het gebruik (of 'misbruik') aangepakt (dat constitueert immers het gronddelict zelf), maar de productie, de handel, het verspreiden en het bezit. Dat het artikel zich richt op de handel is logisch, gezien de gegeven ratio van het aanpakken van een zwarte markt. Het verbieden van productie is in dat licht ook te begrijpen, maar dit is – in elk geval voor

[12] Vgl. Rb. Breda 24 april 2002, LJN-nr. AE1864, *Computerrecht* 2002/ 4, p. 241-3 m.nt. Meijboom, waarin de Auteursrechtrichtlijn pro-actief wordt betrokken in de interpretatie van art. 32a Aw: 'In het licht daarvan dient onder "uitsluitend" ook te worden begrepen elk gebruik dat slechts in geringe mate een ander doel heeft dan het omzeilen van de bescherming.' 'Gering' is minder rekbaar dan 'primair' en daarom een beter hanteerbaar begrip, maar laat nog steeds de nodige interpretatieruimte over.
[13] In Kamervragen over een concept van het Verdrag, waarin nog zeer algemeen en verstrekkend werd gesproken over 'instrumenten die geschikt zijn', antwoordde de regering: 'In de toelichting op het verdrag zal moeten worden verduidelijkt dat het alleen gaat om instrumenten (…) die blijkens hun aard *slechts* geschikt zijn voor crimineel gebruik' (onze cursivering). *Kamerstukken II*, 2000-2001, 23 530, nr. 45, p. 9. Aangezien later echter het woord 'primarily' is ingevoegd in de verdragstekst, vallen er volgens ons geen conclusies aan te verbinden over de huidige intenties van de wetgever op dit punt.

Nederlands recht – wel vergaand. Juist dit bergt het boven gesignaleerde gevaar van verkillend effect op onderzoek en ontwikkeling van ICT in zich.
Het verbod op verspreiding is op zichzelf minder opzienbarend, al vinden wij de opneming van hyperlinks onder verspreiding wel vergaand. De opzeteis zal hier strikt moeten worden gehanteerd: uit de contekst zal ondubbelzinnig moeten blijken dat de verwijzer met de hyperlink het oogmerk had om strafbare hulpmiddelen te verspreiden. Ook vergaand is de strafbaarstelling van bezit van hulpmiddelen. Dit heeft immers weinig van doen met de gegeven ratio van het voorkomen van een zwarte markt, en sluit ook slecht aan op huidige strafbaarstellingen.

Gelukkig kunnen de bovengeplaatste kanttekeningen voor een belangrijk deel gerelativeerd worden door de toevoeging van het laatste element, namelijk het verband met het gronddelict. Er wordt opzet geëist op gebruik voor het doel een computerdelict te plegen, zowel bij de handel als bij het bezit. Hierbij moet wel worden aangetekend dat het verdrag niet verplicht om deze beperking te hanteren: partijen mogen ook verder gaan in de strafbaarstelling. Maar zelfs als zij de opzeteis van het verdrag overnemen, zal veel afhangen van hoe de eis wordt uitgelegd. Zal het opzet mede subjectief worden uitgelegd, zodat kennis van de beweegredenen van de dader nodig is? Of wordt volstaan met geobjectiveerde factoren? In het laatste geval bestaat het gevaar dat dit geen extra bescherming biedt: het opzet zou afgeleid kunnen worden uit het enkele feit dat iemand iets doet met een middel dat primair ontworpen is voor het plegen van een computerdelict, en wat kan iemand anders van zins zijn dan dat middel te gebruiken waarvoor het is ontworpen? Hier mag de subjectieve intentie niet worden weggeobjectiveerd. En vanwege dit belang van de subjectieve intentie moet voorwaardelijk opzet volgens ons hier afgewezen worden: er moet oogmerk bestaan tot het plegen van een computerdelict.

Concluderend hebben wij de nodige bedenkingen bij de voorgestelde strafbaarstelling. De noodzaak van het voorkomen van een zwarte markt wordt onvoldoende gemotiveerd in het licht van de integrale strafbaarstelling van hulpmiddelen, die ook lichte vormen van computercriminaliteit kan betreffen. De reikwijdte van het artikel is groot, onder andere door het omvatten van wachtwoorden en toegangscodes, de vage aanduiding dat het gaat om 'primair' misdadig ontworpen hulpmiddelen, en de strafbaarstelling van vervaardigen, bezit en verspreiden door middel van hyperlinks. Het is de vraag of de aanvullende opzeteis op het plegen van een computerdelict deze brede reikwijdte voldoende kan inperken tot daadwerkelijk strafwaardige voorbereidingshandelingen. Al met al zijn er volgens ons voldoende kanttekeningen voor de Nederlandse wetgever om bij de ratificatie voor dit artikel een voorbehoud te maken.

3.2. Kraakmiddelen en het auteursrecht

Hoewel bij de ontwikkelingen in het Cybercrime-Verdrag de nodige kanttekeningen te plaatsen zijn, blijven de voorstellen op dat terrein zich nog wel grotendeels beperken tot hulpmiddelen met een (hoofdzakelijk) illegale bestemming en tot enige opzet op het plegen van onrechtmatige handelingen. Wanneer we kijken naar technische hulpmiddelen in het auteursrecht, dan lijken zelfs deze ankerpunten voor aansprakelijkstelling op de tocht te staan. Een analyse van deze ontwikkeling is juist daarom van belang omdat, de voorgestelde auteursrechtelijke regeling weliswaar nu een civielrechtelijke sanctie kent, maar de regering beziet hoe de regeling zich verhoudt tot de strafrechtelijke normering van art. 6 CCV.

In ons land werd op 22 juli 2002 een wetsvoorstel ingediend ter aanpassing van de Auteurswet aan de Auteursrechtrichtlijn.[14] In artikel 29a Aw van dit voorstel wordt het maken, aanbieden en verspreiden van kraakmiddelen als onrechtmatig aanmerkt, daarmee art. 6 van de Richtlijn

[14] Richtlijn 2001/ 29/ EG, *PbEG* L 167/ 10, 22 juni 2001.

implementerend.[15] Wat betreft de bestemming van het middel concretiseert dit artikel de omzeilingshandelingen waartegen opgetreden zou moeten worden:

> 'de vervaardiging, invoer, distributie, verkoop, verhuur, reclame voor verkoop of verhuur, of het bezit voor commerciële doeleinden van inrichtingen, producten, onderdelen of het verrichten van diensten die a) gestimuleerd, aangeprezen of in de handel gebracht worden om bescherming te omzeilen, of b) slechts een commercieel beperkt doel of nut hebben, of c) in het bijzonder ontworpen zijn met het doel de omzeiling mogelijk of gemakkelijk te maken van doeltreffende technische voorzieningen.'

De elementen van 'commercieel beperkt doel of nut' en 'in het bijzonder ontworpen met het doel' beogen een onderscheid te maken tussen enerzijds middelen waarvan het doel is om omzeiling mogelijk of gemakkelijk te maken en anderzijds middelen waarvan omzeiling een neveneffect kan zijn (zoals een computer met een grote rekencapaciteit waarmee in principe ook technische beschermingsmiddelen kunnen worden uitgeschakeld).[16] Tussen deze twee uitersten ligt een grijs gebied van middelen die niet uitsluitend een omzeilingsdoel hebben maar waarvan omzeiling wel meer is dan een neveneffect; of dit grijze gebied aan de ene of aan de andere kant zal worden toegerekend, is onduidelijk.
Het volgende element, de intentie waarmee de omzeilingsmiddelen worden ingezet, blijkt irrelevant onder de Richtlijn. Men kiest voor een definitie van beschermde technische voorzieningen die ontkoppeld is van de beschermingsomvang van het auteursrecht. Met andere woorden, omzeiling is verboden, ongeacht of er sprake kan zijn van omzeiling om te kunnen genieten van een wettelijke beperking als het citaatrecht, gebruik voor onderwijsdoeleinden of een recht op een privékopie.[17] De Europese wetgever kiest er daarbij ook niet voor om, naar voorbeeld van de VS,[18] de mogelijkheid te creëren voor toekomstige expliciete kraakexcepties voor legitieme doeleinden. In woorden heeft de Richtlijn oog voor een noodzakelijke balans tussen enerzijds de belangen van rechthebbenden en anderzijds erkende informatievrijheden (overweging 31). Men heeft het echter niet aangedurfd deze woorden om te zetten in daden en aldus ontbreken concrete aanknopingspunten voor het vinden van deze balans.

Een blik op de Nederlandse implementatiebepaling van art. 29a Aw laat zien dat nauw wordt aangesloten bij de tekst van de richtlijn. Zowel de omzeilingshandeling zelf (lid 2) als het vervaardigen, invoeren, verkopen, adverteren, aanbieden en aanprijzen van omzeilingsmiddelen (lid 3) vallen binnen het bereik van de regeling. Bij de omzeilingshandeling zelf haalt het tweede lid het element van intentie binnen, maar in een afgezwakte vorm: 'Degene, die doeltreffende technische voorzieningen omzeilt en dat weet *of redelijkerwijs behoort te weten*, handelt onrechtmatig' (onze cursivering). Aldus is het omzeilen van een beveiliging alleen onrechtmatig als dit met opzet of culpa gebeurt. Maar daarmee is de kou niet uit de lucht: het bewust omzeilen van een beveiliging is namelijk ook onrechtmatig als dit geschiedt met het oogmerk een rechtmatige handeling te kunnen verrichten.[19] Hetzelfde geldt voor de voorbereidingshandelingen van lid 3. Een cryptograaf die omzeilingsmiddelen ontwikkelt of daar tijdens een congres de aandacht op

[15] *Kamerstukken II* 2001/ 02, 28 482, nrs. 1-3. Zie eerder over deze regeling: K.J. Koelman, 'Bescherming van technische voorzieningen', *AMI* 2001-1, p. 16-27, en meer algemeen over technische voorzieningen Koelmans publicaties op <http:/ / www.ivir.nl/ publicaties/ intellectuele-eigendom.html>.
[16] Zie p. 58 MvT bij het Nederlandse implementatievoorstel: Kamerstukken II 2001/ 02, 28 482, nr. 3.
[17] Zie ook het antwoord van de Minister naar aanleiding van een vraag van de VVD-fractie, *Kamerstukken II* 2002/ 03, 28 482, nr. 8, p. 18.
[18] Op grond van afdeling 1201(a)(1)(B)-(D) van de DMCA kunnen elke twee jaar bij het Copyright Office uitzonderingen (*exemptions*) worden aangevraagd op het omzeilingsverbod. Tot op heden heeft het Copyright Office zich zeer spaarzaam getoond in het afkondigen van uitzonderingen. Zie D. L. Burk & J.E. Cohen, 'Fair Use Infrastructure for Rights Management Systems', *Harvard Journal of Law & Technology* Fall 2001, p. 41-83.
[19] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 58.

vestigt met als oogmerk om in het kader van zijn onderzoek te wijzen op bepaalde beveiligingslekken in systemen handelt onrechtmatig.[20]
De vanuit de Europees onmacht doorgeschoven opdracht aan de lidstaten om in 'passende maatregelen' te voorzien die ervoor zorgen dat gebruikers een beroep kunnen blijven doen op de bekende beperkingen op het auteursrecht (art. 6 lid 4 sub 1 Auteursrichtlijn) wordt vooralsnog niet uitgevoerd. Het heikele punt is overgelaten aan een eventuele algemene maatregel van bestuur; de minister van Justitie heeft aangegeven pas te zullen ingrijpen op het moment dat de betekenis en de ratio van de beperkingen in het gedrang komen.[21] Tot dat moment zal ook de inzet van omzeilingssystemen met het oog op het verrichten van een in principe rechtmatige verveelvoudigingshandeling als een onrechtmatige daad conform art. 29a Aw worden aangemerkt.
In 2001 stelde de Commissie Auteursrecht voor het inbreukelement te verweven in de definitie van technische voorzieningen.[22] Daarmee beoogde zij een directere relatie te leggen met het oogmerk van de inbreuk op een auteursrecht en zo door de wet toegelaten gebruikshandelingen buiten schot te houden. De regering betoogt dat de Richtlijn geen ruimte laat voor deze optie.[23] Daarmee wordt duidelijk dat het spel in Europa is gespeeld en posities niet opnieuw kunnen worden betrokken.[24] In antwoord op vragen uit het parlement stelt de regering: 'wat er ook zij van de eventuele wenselijkheid hiervan [het opnemen van uitzonderingen voor bepaald rechtmatig gebruik, onze toevoeging], vastgesteld moet worden dat de richtlijn daarin niet voorziet. (...) [H]et is de regering niet toegestaan om hierop eenzijdig een uitzondering te introduceren.'[25] De meer fundamentele discussie over de implicaties van deze internationale normstelling vanuit een oogpunt van de systematiek van het nationale (auteurs)recht en – mocht het in de toekomst mogelijk tot een strafrechtelijke handhaving komen (zie onder) – van het materiële strafrecht gaat de regering uit de weg.

Het auteursrechtbeleid in het ICT-tijperk kiest dus voor een duidelijke koerswijziging: alhoewel er inherent niets mis hoeft te zijn met een hulpmiddel (de omzeilingsfaciliteit), worden alle handelingen daarmee verboden. De bestemming van het hulpmiddel wordt geheel losgekoppeld van onrechtmatigheid. Een vergaande stap daarbij is voorts dat de intentie van het gebruik geen rol speelt. Of de handeling nu met of zonder legitiem oogmerk plaatsvindt, zij is verboden. Aldus wordt het hulpmiddel in abstracto en in concreto feitelijk onrechtmatig verklaard, zonder band met een onderliggende strafwaardige gedraging.
Het is de vraag of een dergelijke maatregel proportioneel is in het licht van de belangen die worden geraakt en of deze past binnen het auteursrechtstelsel en de achterliggende ratio daarvan. Los van het antwoord hierop, is voor het onderwerp van deze bijdrage relevant wat de implicaties van de regeling zijn voor de strafbaarstelling van hulpmiddelen. Alhoewel de wetgever

[20] De Nederlandse cryptografie-deskundige Niels Ferguson die onderzoek doet naar zwakke onderdelen van encryptie van video-signalen, publiceerde zijn onderzoeksresultaten niet in het Engels uit angst voor vervolging in de VS op grond van de DMCA. Ook onder het Nederlandse wetsvoorstel zou hij in de problemen kunnen komen: de minister heeft aan de Tweede Kamer (nr. 5, p. 42) weliswaar toegezegd dat art. 29a 'serieus' cryptografisch onderzoek niet mag verhinderen, maar hij heeft niet aangegeven wanneer onderzoek 'serieus' kan worden geacht. Zie hierover de brandbrief van diverse experts aan de Tweede Kamer, beschikbaar op <http:/ / www.bof.nl/ auteursrecht.html>. Zie ook *Kamerstukken II* 2001/ 02, 28 482, nr. 7, p. 15.
[21] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 58. Zie tevens p. 28-31. De vraag is natuurlijk in hoeverre de Nederlandse regering invloed heeft op informatieaanbieders uit landen van buiten de EU en hen via een AMvB kan verplichten recht te doen aan wettelijke gebruiksrechten.
[22] Zie hierover *Kamerstukken II* 2001/ 02, 26 538, nr. 5.
[23] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 55.
[24] Een evaluatie van de Richtlijn is aangekondigd voor uiterlijk eind van dit jaar (2004), maar het valt – gezien het precaire compromiskarakter van de richtlijn – niet op voorhand te verwachten dat de richtlijn op dit punt fundamenteel zal worden gewijzigd.
[25] *Kamerstukken II* 2002/ 03, 28 482, nr. 8, p. 5.

vooralsnog kiest voor een civielrechtelijke handhaving,[26] blijkt uit de MvT dat de wetgever zal bezien hoe deze situatie zich verhoudt tot de strafrechtelijke normering van art. 6 Cybercrime-verdrag.[27] Het is daarbij ook opvallend met welk een eenvoud leden van enkele kamerfracties, in navolging van de Raad van State,[28] de suggestie hebben aangedragen te kiezen voor handhaving langs de strafrechtelijke weg. Immers, zo is de redenering, de handelingen neergelegd in art. 29a Aw zullen 'na ratificatie van het Verdrag inzake Cybercrime, ingevolge art. 6 van dat verdrag, (deels) strafbaar (...) moeten worden gesteld'. De Minister hield tot dusverre gelukkig het hoofd koel en heeft aangegeven dat de materie die het voorgestelde art. 29a Aw beoogt te bestrijken reeds grotendeels wordt afgedekt door de strafrechtelijke bepalingen inzake computervredebreuk (art. 138a Sr), listig gebruik maken van een telecommunicatiedienst (art. 326c Sr) en het manipuleren van gegevens (art. 350a Sr). Mede vanwege de verscheidene open normen die zijn opgenomen in art. 29a Aw (zoals 'doeltreffende' technische voorzieningen, normale werking en een commercieel beperkt doel of nut) geeft de Minister er de voorkeur aan 'dat thans eerst ervaring wordt opgedaan met de nieuwe artikelen en de bestaande en in voorbereiding zijnde nieuwe strafrechtelijke instrumenten en dat vervolgens wordt beslist of andere handelingen binnen het bereik van art. 29a strafbaar moeten worden gesteld met een daarop toegesneden strafmaat.'[29] De Minister is echter geen principiële tegenstander van strafrechtelijke handhaving.[30]

Beoordeling

Alhoewel de regeling van art. 29a Aw vooralsnog geen strafrechtelijke sanctie kent, is het bepaald niet uitgesloten dat in de toekomst ook via het strafrecht gehandhaafd zal worden. In hoeverre zou dan de aansprakelijkheid voor omzeilingsmiddelen in het systeem van de strafwet passen? Wederom is dus de eerste vraag wat de reden is voor een verbod op omzeilingsmiddelen. Deze vraag is mede van belang nu de geïntroduceerde regeling volstrekt vreemd is aan het systeem van de Auteurswet.[31] De MvT merkt op dat de regeling 'gerechtvaardigd wordt door de investeringen die nodig zijn om de technische voorzieningen op communautair niveau te ontwikkelen, de problemen rond handhaving van auteursrecht in de digitale omgeving en de wens om van de mogelijkheden die de techniek biedt, zo ruim mogelijk gebruik te maken.'[32] Kortom, het verbod op omzeiling heeft allereerst expliciet tot doel de compatibiliteit en interoperabiliteit op de nog jonge markt van technische beschermingsmiddelen te bevorderen. 'Tegelijkertijd is de bescherming tegen handelingen en apparatuur die omzeiling mogelijk maken ook bedoeld als zekerheid voor bedrijven die zich toeleggen op de productie van hardware en die investeringen doen om nieuwe beschermingstechnieken in te bouwen of te herkennen dat niet anderen deze technieken zonder moeite kunnen doorbreken.'[33]

Een tweede overweging is gelegen in de wens tot een meer effectieve handhaving. Het is onmiskenbaar dat juist in de digitale omgeving het handhavingsvraagstuk op scherp is komen te staan. Juist om te komen tot een verhoogde effectiviteit van het bestrijden van auteursrechtinbreuken omvat het verbod van art. 29a Aw behalve het gebruik van de omzeilingsfaciliteit als zodanig, ook allerlei handelingen die dienen ter voorbereiding van de

[26] Dit mede gelet op het feit dat de strafnorm van art. 32a Aw in de praktijk bezwaarlijk toepassing vindt en de Richtlijn genoegen neemt met enkel civielrechtelijke sanctionering, aldus de MvT (p. 56).
[27] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 27. Zie ook p. 56.
[28] De Raad van State meende dat de regering onvoldoende duidelijk maakt waarom een strafrechtelijke handhaving in de praktijk op bezwaren stuit, en hij wijst op de inconsequentie ten gevolge van het verschil in handhaving van art. 32a Aw (het strafbaar gestelde omzeilen van beveiliging bij computerprogrammatuur). *Kamerstukken II* 2001/ 02, 28 482, B, p. 8-9.
[29] *Kamerstukken II* 2002/ 03, 28 482, nr. 5, p. 41.
[30] *Handelingen II* 11 februari 2004, 50-3338.
[31] Ook de wetgever onderkent dat met de regeling een nieuwe vorm van bescherming wordt geïntroduceerd die zich tot een ander terrein uitstrekt dan de klassieke betekenis van het auteursrecht. *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 57.
[32] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 27.
[33] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 28.

daadwerkelijke omzeiling: 'het niveau van bescherming [zou] onvoldoende (...) zijn als slechts het daadwerkelijk omzeilen onrechtmatig is'.[34] Kortom, de ratio van de regeling rondom de voorbereidingshandelingen lijkt mede te zijn gelegen in de ontoereikendheid van een verbod op de omzeilingshandeling zelf. Handhaving is aldus direct redengevend vanwege de moeilijke opspoorbaarheid en vervolgbaarheid van het gebruik van omzeilingsfacilteiten. De regering verwoordt een en ander door op te merken dat gelaedeerden doorgaans het meeste belang hebben bij het aanpakken van de bron.[35] Immers, het is eenvoudiger en effectiever een importeur of aanbieder van omzeilingsapparatuur op te sporen dan een individuele gebruiker die in of vanuit de beslotenheid van de studeerkamer een beveiligingssysteem kraakt – nog afgezien van de privacyimplicaties die een aanpak op het individuele niveau van gebruik met zich mee zal brengen. Uiteindelijk weegt daarmee het economisch (en in het verlengde daarvan, het maatschappelijk) belang zwaarder dan een beperking van het verbod op gebruik van het omzeilingsmiddel. In het licht van bestaande strafbaarstellingen van hulpmiddelen, leveren de huidige handhavingsproblemen waar het auteursrecht mee wordt geconfronteerd op het eerste gezicht een dringende reden op om niet alleen het gebruik, maar ook voorbereidingshandelingen te verbieden.

Opvallend is verder dat de regering de wens om zo ruim mogelijk gebruik te maken van de mogelijkheden die de techniek voor handhaving biedt, expliciet aan de regeling ten grondslag legt. Dit vertrouwen is des te meer opvallend nu de regering zelf onderkent dat deze voorzieningen, althans op dit moment, nog niet in staat zijn in te spelen op het zorgvuldig vormgegeven auteursrechtelijk systeem van machtsevenwicht. Het gegeven dat de techniek momenteel niet in staat is een onderscheid te maken tussen omzeiling voor rechtmatige doeleinden enerzijds en omzeiling met het oog op onrechtmatig handelen anderzijds, in combinatie met de overweging dat de verleiding van misbruik wel heel snel op de loer ligt,[36] vormen voor de wetgever de rechtvaardiging te kiezen voor een systeem van alles of niets.[37]

De vormgeving van het civielrechtelijke verbod op voorbereidingshandelingen met kraakmiddelen is opmerkelijk als we kijken naar de aanknopingspunten voor strafrechtelijke aansprakelijkstelling. In de eerste plaats wordt niet alleen aangeknoopt bij voorwerpen (en alles wat daarop lijkt), maar ook bij dienstverlening (lid 3). In de bestaande strafrechtelijke aansprakelijkstellingen komt dienstverlening als zodanig niet voor.

De bestemming van de hulpmiddelen kent voorts een interessante driedeling. Ten eerste is de bestemming van de middelen zelf (dus in abstracto) irrelevant als zij in concreto worden aangeboden met als doel omzeiling (lid 3 onder a). Indien er dus een oogmerk is om de gewraakte grondhandeling (het omzeilen) te plegen, kan de bestemming van het voorbereidingsmiddel achterwege blijven. Opmerkelijk is dat hier zelfs niet de eis wordt gesteld van geschiktheid: als iemand middelen aanbiedt met als doel omzeiling maar die evident ongeschikt zijn voor omzeiling, handelt hij niettemin onrechtmatig.

Ten tweede gaat het om hulpmiddelen die 'slechts een commercieel beperkt doel of nut hebben anders dan het omzeilen' (lid 3 onder b). Dit is kennelijk iets anders dan de derde mogelijkheid: hulpmiddelen die 'vooral ontworpen, vervaardigd of aangepast worden met het doel het

[34] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 28.
[35] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 58.
[36] 'De bevoegdheid om een voorziening te omzeilen om van een beperking gebruik te maken, zal doorgaans slechts met middelen geschieden die ook een verdergaande omzeiling mogelijk maken, waardoor zo'n bevoegdheid zich makkelijk laat misbruiken.' *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 55.
[37] *Kamerstukken II* 2001/ 02, 28 482, nr. 3, p. 55.

omzeilen' (lid 3 onder c). Dit derde criterium is vergelijkbaar met dat uit het Cybercrime-verdrag, waarop zoals we aangaven het nodige valt af te dingen (zie boven).[38]
De toevoeging van de tweede mogelijkheid ten opzichte hiervan geeft echter aan dat de onrechtmatigverklaring hier nog veel verder gaat: ook middelen die niet ontworpen zijn voor omzeiling maar die (achteraf) een commercieel beperkt nut blijken te hebben, worden onrechtmatig. Dat betekent dat iemand die een hulpmiddel ontwikkelt met als doel informatiebeveiliging, achteraf aansprakelijk kan worden gesteld als het middel commercieel flopt maar door het muziekliefhebberscircuit wordt omarmd voor omzeiling. De onderzoeker en ontwikkelaar moeten kennelijk ervoor zorgen dat de middelen in elk geval potentieel commercieel uit te nutten zijn. Wat deze clausule evenwel nog prangender maakt, is dat een element van opzet of schuld ontbreekt: anders dan onder a en c ('met het doel') hoeft de dader zich niet bewust te zijn van de eigenschap dat de middelen slechts een commercieel beperkt nut of doel hebben anders dan omzeiling. Hierdoor ontstaat een risicoaansprakelijkheid op onderzoek en ontwikkeling van beveiligingstechnieken.
De extremiteit van de aldus vormgegeven bestemming wordt mede veroorzaakt door de ruime opsomming van handelingen die worden verboden: vervaardigen, invoeren, distribueren, verkopen, verhuren, adverteren of voor commerciële doeleinden bezitten. Met name het verbod op vervaardigen is gevaarlijk, zoals we bij art. 6 CCV ook al constateerden.[39] Verder valt op dat het doorvoeren en uitvoeren niet wordt verboden (zou het niet erg zijn als Amerikanen of Aziaten wél illegaal Europese cd's kunnen afspelen?). Het bezit wordt als zodanig niet aangepakt; slechts het bezit voor commerciële doeleinden wordt verboden. Op dit punt gaat de bepaling minder ver dan art. 6 CCV, die ook verbod op bezit van een enkel privé-exemplaar toelaat.

Waar het Cybercrime-verdrag echter de bepaling inperkt door toevoeging van de eis van opzet op het plegen van een computerdelict, blijft in art. 29a de relatie met een in zichzelf onrechtmatige handeling (zoals inbreuk op auteursrecht) achterwege. Het verbod is niet gericht op inbreuken op het auteursrecht, maar op tegengaan van omzeiling van technische bescherming. De ratio is immers het stimuleren van technische beschermingsvoorzieningen. Voor dit beleidsmatige, economische doel wordt het middel gehanteerd van een civielrechtelijk verbod op een handeling die in zichzelf niets onrechtmatigs hebben maar die afbreuk kunnen doen aan dit doel. Het is sterk de vraag of dit middel wel voldoet aan de eisen van subsidiariteit en proportionaliteit. Een strafrechtelijk verbod zou voor dit doel in elk geval uit den boze zijn, aangezien het verbod allerminst als ultimum remedium kan worden beschouwd. Maar ook voor een civielrechtelijk verbod lijkt het ons een paardenmiddel: zou men niet eerst andere, minder ingrijpende reguleringsinstrumenten moeten beproeven, zoals fiscale stimulering, voorlichtingscampagnes en stimulering van wetenschappelijk onderzoek naar technische beschermingsvoorzieningen?

4. Conclusie en aanbevelingen

De besproken ontwikkelingen in strafbaarstelling van ICT-gerelateerde hulpmiddelen zijn vergaand. Zij dreigen de grens van strafrechtelijke aansprakelijkheid nog verder naar voren te verschuiven, terwijl deze grens door diverse bijzondere strafbaarstellingen, maar vooral door het algemene verbod op voorbereidingshandelingen van art. 46 Sr, al een behoorlijk eind lag vóór het

[38] De formulering wijkt af door te spreken van 'ontworpen, vervaardigd of aangepast *worden*' (onze cursivering), waar art. 6 CCV alleen het deelwoord 'designed' gebruikt, dat wil zeggen 'ontworpen worden of zijn'. Taalkundig zou men art. 29a lid 3 onder c kunnen interpreteren als alleen omvattend de ontwikkelfase van hulpmiddelen; zodra een hulpmiddel af is, zou het dan niet meer onder deze grond voor aansprakelijkheid vallen. Dit wijkt dermate af van de richtlijn (die 'zijn' gebruikt), dat wij ervan uitgaan dat 'worden' moet worden gelezen als 'zijn'.
[39] In de Tweede Kamer is voorgesteld de clausule 'voor commerciële doeleinden' (die nu alleen bij bezit staat) op alle voorbereidingshandelingen van toepassing te verklaren, zodat de reikwijdte zou worden ingeperkt. De Minister heeft het amendement ontraden vanwegen strijd met de richtlijn. *Kamerstukken II* 2003/ 04, 28 482, nr. 16; *Handelingen II* 11 februari 2004, 50-3347.

voorportaal van strafwaardig gedrag. Deze verschuiving wordt veroorzaakt door het brede bereik van de voorstellen. Zo omvat art. 6 Cybercrime-verdrag niet alleen hulpmiddelen in eigenlijke zin, maar ook wachtwoorden en toegangscodes; het Nederlandse strafrecht kent, met uitzondering van de telecomfraude (art. 326c lid 2 Sr), geen precedent voor voorbereidingshandelingen met dergelijke computergegevens. Het voorgestelde art. 29a Auteurswet geldt élke omzeiling, ongeacht het doel. De onderbouwing van deze voorstellen kan op zijn best matig worden genoemd: nergens wordt afdoende gemotiveerd waarom een dergelijke brede aanpak noodzakelijk is.
Hoe men ook overigens de afweging om over te gaan tot strafbaarstelling beoordeelt, op enkele onderdelen schieten de voorstellen in elk geval te ver door. Het voorgestelde art. 29a lid 3 onder b Aw stelt aansprakelijk voor hulpmiddelen met een beperkt commercieel doel of nut, ongeacht of de dader zich daarvan bewust was; hier zou, zoals bij de andere onderdelen van lid 3, ook een element van 'met het doel omzeiling te faciliteren' moeten worden opgenomen. Verder is de reikwijdte van art. 29a Aw dusdanig ingrijpend (namelijk ongeacht enige inherente onrechtmatigheid), dat in elk geval strafrechtelijke sanctionering sterk afgewezen moet worden. Tot slot staat de strafbaarstelling van voorbereidingshandelingen voor computerdelicten los van de ernst van het voorgenomen delict; in het Nederlandse systeem – waar strafbare voorbereiding nog steeds een uitzondering hoort te zijn – wordt alleen voorbereiding van ernstige, gevaarzettende feiten aangepakt. Bij de implementatie zou Nederland daarom in elk geval de opzeteis moeten relateren aan de ernstige, gekwalificeerde vormen van computercriminaliteit.

Als de aansprakelijkstellingen onverkort worden doorgezet, zullen tal van handelingen met nieuwe technologie onder het bereik komen van verbodsbepalingen, ook als zij geen primaire of slechts een zeer indirecte relatie hebben met strafwaardig gedrag. De voorstellen versterken duidelijk de tendens van instrumentalisering van het strafrecht die de literatuur al eerder signaleerde bij de leerstukken van poging en voorbereiding aan het eind van de twintigste eeuw.[40] Nu is instrumenteel denken niet altijd af te wijzen, maar men moet zich wel bewust zijn van het gevaar dat fundamentele uitgangspunten geleidelijk kunnen worden uitgehold, met name door cumulatie van vele, elk op zich kleine instrumentele maatregelen.
De instrumentalisering past binnen de brede tendens van, zoals Gutwirth en de Hert het noemen, 'penalisering van de samenleving' die bestaat uit 'inflatie aan strafbepalingen en (...) overbevraging van het strafrecht vanuit de samenleving'. Zij waarschuwen ervoor dat dergelijke ontwikkelingen 'het strafrecht banaliseren, eroderen en ontwaarden.'[41]

Wellicht zal de wetgever ons tegenwerpen dat hij niet zelf kiest voor deze aanpak, maar door internationale regelgeving wordt gedwongen tot het oprekken van het voorveld van strafrechtelijke aansprakelijkstelling. Voor een deel is dat waar – maar slechts voor een deel. De dreiging komt ook van binnenuit, zoals de per 1 januari 2004 van kracht geworden strafbaarstelling van radarverklikkers in het verkeersstrafrecht laat zien. Belangrijker nog is dat de wetgever nogal eens gemakzuchtig lijkt te zijn in de implementatie van supranationale regelgeving.[42] De auteursrechtrichtlijn laat weliswaar niet veel speelruimte, maar in de interpretatie lijkt de wetgever wel erg volgzaam. Volgens ons kan de wetgever zeker meer ruimte nemen om bepaalde onderdelen van art. 6 Richtlijn te interpreteren in een richting die minder risico oplevert voor de ontwikkeling en het gebruik van technische hulpmiddelen, bijvoorbeeld

[40] Getuige zijn conclusie 'dat wetgever en rechtspraak tegenwoodig gemakkelijker, instrumenteler en ruimer omgaan met algemene leerstukken van strafrechtelijke aansprakelijkheid (...). Praktisch werkbare uitkomsten vormen een belangrijke toetssteen, dogmatische en systematische vragen zonder praktische ondergrond krijgen minder aandacht.' De Hullu, *a.w.*, noot 8, p. 410.
[41] S. Gutwirth & P. De Hert, 'Een theoretische onderbouw voor een legitiem strafproces', *Delikt & Delinkwent* 2001/ 10, p. 1076-1077.
[42] Vgl. E.A.M. Verheijen & L. Stevens, 'Nationale waardenoriëntatie in strafrechtelijk Europa', in: *Glijdende Schalen*, a.w., noot 1, p. 575-590.

door in de toelichtende teksten meer oog te hebben voor het rechtmatig gebruik van omzeilingstechnieken, en door scherper aan te duiden waar de aansprakelijkstelling in elk geval moet ophouden. Ook is de afwachtende houding bij het waarborgen van de wettelijke beperkingen op het auteursrecht niet noodzakelijk: de richtlijn staat hier een actiever en tijdiger ingrijpen toe.[43]
Bij het Cybercrime-verdrag valt te hopen dat de nationale wetgever zich minder verschuilt achter de internationale afspraak en meer oog heeft voor het eigen systeem van het strafrecht. Het verdrag biedt ook de ruimte een voorbehoud te maken bij artikel 6. De wetgever moet die mogelijkheid serieus in overweging nemen en in elk geval art. 6 niet in de gehele brede reikwijdte implementeren. De strafbaarstelling zou zich volgens ons moeten beperken tot de minimumeisen van het verdrag: de verkoop, verspreiding of beschikbaarstelling van wachtwoorden, toegangscodes of soortgelijke gegevens waarmee toegang kan worden verkregen tot een computersysteem met het oogmerk dat deze gebruikt worden om een cyberdelict te plegen. Het meest praktisch lijkt ons daartoe een apart artikel op te nemen in het Wetboek van Strafrecht. Een 'cyberdelict' zou daarbij moeten worden beperkt tot de ernstige vormen van computercriminaliteit, dat wil zeggen gekwalificeerd hacken (art. 138a lid 2-3), gekwalificeerde gegevensmanipulatie (art. 350a lid 2-3), opzettelijke computersabotage (art. 161sexies, 351) en onderscheppen van telecommunicatie (art. 139c) of van besloten gegevensoverdracht (art. 139a lid 2).

Meer in het algemeen vinden wij dat zowel de wetgever als het parlement zich kritisch moeten opstellen bij strafbaarstelling van technische hulpmiddelen, kritischer dan zij tot nu toe blijken te zijn. In plaats van bij technische ontwikkelingen te grijpen naar het paardenmiddel van een ongenuanceerd verbod, zouden zij meer aandacht moeten besteden aan de diverse functies die de nieuwe technologie kan hebben en aan de hand daarvan een scherper en transparanter afbakening moeten maken van wat precies wordt verboden. Daarbij moet er meer oog zijn voor de gevolgen die een verbod heeft voor de ontwikkeling van nieuwe technologie, maar ook voor de fundamenten van het strafrecht en het auteursrecht, met inachtneming van de mogelijke cumulatie van aansprakelijkstellingen. En men moet beter motiveren waarom een verbod noodzakelijk is en waarom niet kan worden volstaan met andere, minder ingrijpende reguleringsinstrumenten, of waarom niet kan worden afgewacht tot meer duidelijkheid is verkregen over de implicaties van de technische ontwikkelingen.[44] Kortom, het debat over aansprakelijkstelling van technische hulpmiddelen moet, ook als deze 'uit Europa' komt, in elk geval resulteren in een beredeneerde en gemotiveerde keuze. En moge het debat dat tot die keuze leidt niet worden beheerst door technofobie en instrumentele gemakzucht, maar door kennis van zaken en waardering voor de fundamentele belangen van het recht.

[43] Vergelijk de in noot 18 besproken aanpak van de Amerikaanse wetgever in afdeling 1201 *Digital Millennium Copyright Act*.
[44] Zo concludeerde een door de Canadese regering gepubliceerd rapport dat Canada vooralsnog niet moet overgaan tot een aansprakelijkheidstelling voor omzeilingstechnieken, omdat onvoldoende duidelijk is welke implicaties technische beschermingsmaatregelen zullen hebben op de balans van rechten en beperkingen die inherent is aan het auteursrechtsysteem. Zie: I. Kerr, A. Maurushat & C.S. Tacit, *Technical Protection Measures. Part II. The Legal Protection of TPMs*, 2002, beschikbaar via <http:/ / www.pch.gc.ca/ progs/ ac-ca/ progs/ pda-cpb/ pubs/ index_e.cfm>.